5-5　電子時刻認証システム開発

5-5 Development of the Trusted Time Stamping System

岩間　司　　栗原則幸　　今江理人　　今村國康　　小竹　昇　　後藤忠広
鈴山智也　　森川容雄
IWAMA Tsukasa, KURIHARA Noriyuki, IMAE Michito, IMAMURA Kuniyasu,
KOTAKE Noboru, GOTO Tadahiro, SUZUYAMA Tomonari, and MORIKAWA Takao

要旨

近年、電子商取引の発展やe-Japan重点計画に見られる高度情報通信ネットワーク社会の構築に伴う流通情報の電子化が盛んになってきている。情報の電子化に伴う様々な問題は電子署名技術だけでは対応することが難しい。これらの問題を解決するためには、署名に加え保証された正確な時刻を付与することにより解決できる。本稿では、通信総合研究所（CRL）が日本標準時の供給のみではなく、供給した時刻を証明する国家時刻標準機関として活動するために必要となる時刻認証システムの開発と今後の予定について述べる。

IT social infrastructures based on the "e-Japan Strategy" and the development of e-commerce are rapidly increasing. Acoording to this trend, documents are changing from paper-based to digital data. If we use only digital-signature techniques for digital data, it is difficult to guard against fraudulent practices. We have found that time stamping techniques, which, when combined with digital signatures, provides an effective solution to this problem. In this paper, we present the results of our basic time-transfer measurements and future plans, which are needed by the National Time Authority.

[キーワード]
国家時刻標準機関，標準時配信事業者，タイムスタンプサービス事業者
National time authority, Time authority, Time stamping authority

1　はじめに

近年、電子商取引の発展やe-Japan重点計画に見られる高度情報通信ネットワーク社会の構築に伴う流通情報の電子化が盛んになってきている。このような電子化された情報を取り扱う際に避けられない問題として、他人のなりすましや文書の改ざんを防止すること、また、事実が発生したこと自体を後で否定する事後否認などの問題がある。これらの対策として電子署名技術などが盛んに研究されたが、電子署名技術だけではこれらに対応することが難しい。例えば、申請や受付などを行った場合の正確な時刻情報がないために存在証明が難しい、他人の改ざんは防止できても本人による書換えは可能である、また公開鍵の有効期限の関係から文書の長期保存が難しいなどの問題が残されている。これらの問題に対しては、署名に加えて保証された正確な時刻を付与することにより解決できる。この保証された正確な時刻を付与する技術が電子時刻認証技術である。

CRLは、時間・周波数の供給に責任を有する機関として、これまでUTCにトレーサブルな日本標準時を維持・供給してきた。ところがこれまでは、正確な時刻を供給するのみで供給した時刻の保証は行っていなかった。

現在、事業としての時刻認証システムは既に稼動しているが、いずれもGPS等を時刻源としているため、日本標準時を時刻源としたいという要求が高まっている。これらの状況から、CRLとしてもUTCにトレーサブルな日本標準時を供給するのみではなく供給した時刻を証明す

る、国家時刻標準機関（National Time Authority : NTA）としての活動を開始する必要がある。

本稿では、NTAとして活動するために必要となる時刻認証システムの開発と今後の計画について述べる。

2 時刻認証システムの概要[1]

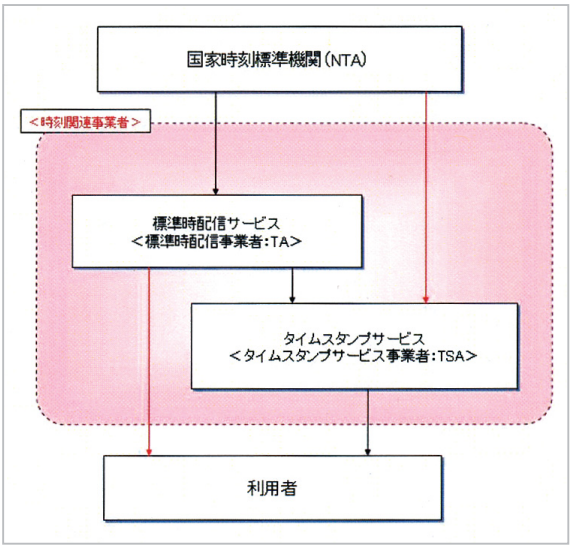


図1 電子時刻認証システムのイメージ

我々の想定する時刻認証システムのイメージを図1に示す。ここで標準時配信事業者（Time Authority：TA）及びタイムスタンプサービス事業者（Time Stamping Authority：TSA）は信頼できる第三者機関（Trusted Third Party：TTP）である。これまでの時刻供給と大きく異なる部分は、NTAがTAやTSAに時刻を供給するだけではなく、その時刻を監査して証明書を発行する部分である。この部分のNTAとしての役割についてまとめたのが図2である。ここで赤い矢印で示してある部分が電子時刻認証システムを実施する上で新たに生じた責任部分である。この部分についてどのようにして実現していくかが電子時刻認証システム開発のNTAとしての課題である。これは大きく分けると三つの課題となる。

・セキュリティの確保
・時刻精度の確保
・証明書の発行とログの保存

これらについて現在、市販されているシステムを改造して時刻配信に関する基礎実験を実施した。これについて次に述べる。

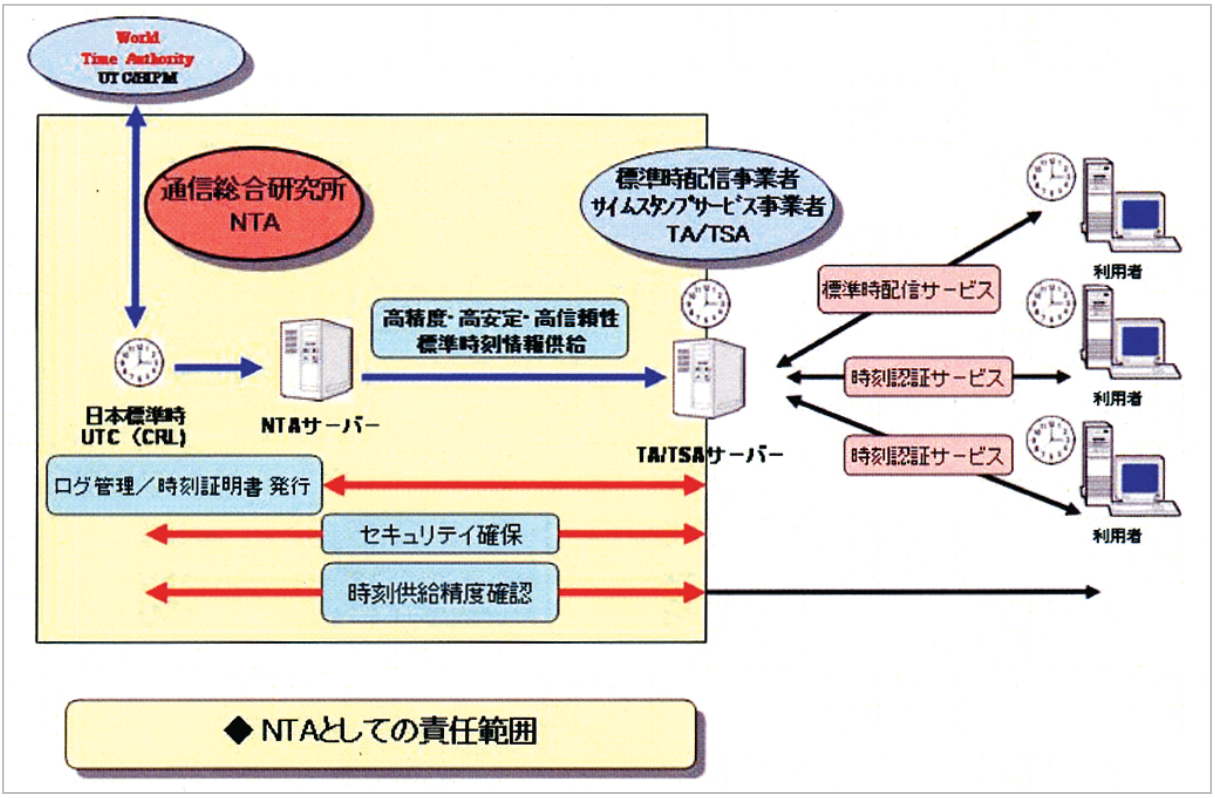


図2 NTAとしての責任範囲

3　標準時供給評価基礎実験[2]

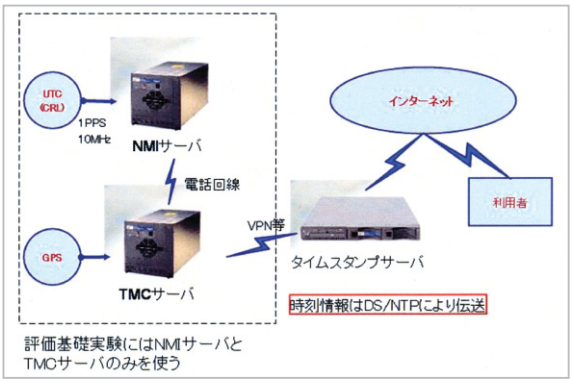


図3　標準時供給評価実験システム

実施した標準時供給評価基礎実験のシステム構成を図3に示す。今回使用したNMIサーバ及びTMCサーバは、Datum社（現Symmetricom社）のTrusted Time Systemを用いた。これらのサーバは、内部時計としてルビジウム発振器を内蔵しており、NMIサーバはUTC（CRL）と同期をとり、TMCサーバはGPSを基準として時計を運用しNMIサーバから電話回線を経由して時刻同期をとる。

現在、計算機等で時刻同期を実現するために最も一般的な方法としてNTP（Network Time Protocol）という手法がある。この評価基礎実験用のシステムでは、DS/NTPというDatum社が開発したセキュアな時刻伝送プロトコルを用いている。また、電話回線を用い、認証基盤として公開鍵認証基盤（Public Key Infrastructure：PKI）を用いることにより、更にセキュリティを確保している。

評価基礎実験用システムを用いて時刻配信実験を行い、測定した結果の一例を図4に示す。今回の測定では、UTC（CRL）とNMIサーバを直接接続し、NMIサーバとTMCサーバは回線シミュレータを介して電話回線で接続した。図4の黄色で示している点がNMIサーバとTMCサーバの時刻差である。

TMCサーバのカタログスペックは時刻同期精度10ms以内である。図4から、時刻差は0.1msであり、このスペックを満足していることが分かる。

時刻配信実験は、シミュレータによって遅延時間を変化させたり、実際にNTTの電話回線を利用して測定したが、測定結果に有意な差はなく、本評価基礎実験用システムを用いることにより精度10ms以内でのセキュアな時刻配信が可能であることが分かった。しかし、本実験は時刻配信についての検証であり、時刻認証に関する検討は未実施である。

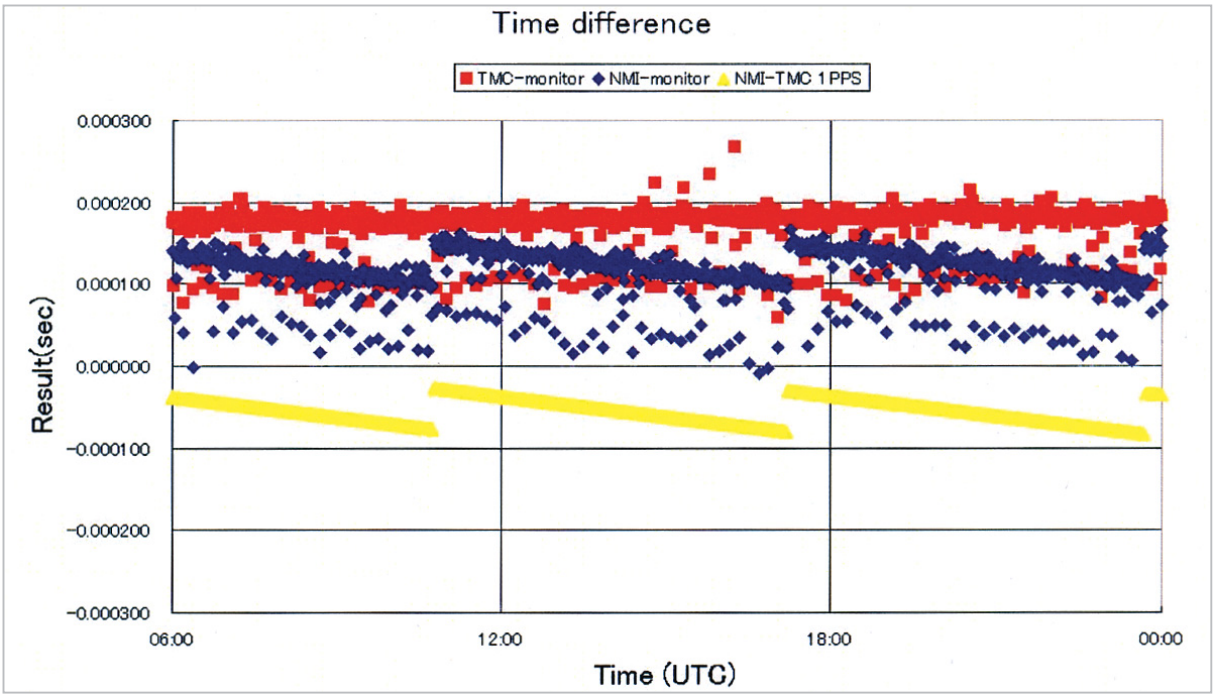


図4　時刻配信実験の測定結果

4　今後の検討

3では、セキュアな時刻配信実験について述べた。これにより、**2**で示した課題のうち「セキュリティの確保」及び「時刻精度の確保」についての一方法が確認できた。しかし、我々がNTAとして事業を行うためには、配信された時刻を検証する必要がある。

配信された時刻の検証には、**5-4-2**で開発を進めている遠隔校正装置が有効である。遠隔校正装置を用いてTA/TSAに供給された時刻の正確さを検証する仕組みを構築し、これを元に時刻認証を行い、「証明書の発行とログの保存」という3番目の課題の解決を図る。以上のことから、時刻認証システムの実用化に向けて以下の項目について検討を行う必要がある。

・遠隔校正装置を用いた時刻検証方法
・時刻認証頻度
・証明書発行方法
・ログの取扱い

これらについては、タイムビジネス推進協議会などを通じてTA/TSAの事業者と検討を行っていく。

また、今回の実験は時刻配信手法の一方法にしか過ぎない。今後とも様々な時刻配信手法について検討を行っていく必要がある。

5　まとめ

ここでは、電子時刻認証システムの開発について、解決すべき三つの課題とCRLにおけるこれまでの取組及び今後検討すべき項目について述べた。解決すべき課題については、どのような形で実施していくか、また、これらがTA/TSAから利用者までに伝達されるためにはどのようにしたらいいか、タイムビジネス推進協議会などを通じてTA/TSAの事業者と今後も検討を深めていく[3]。

また、時刻配信について一方式における検証を実施したが、時刻認証に関する検討は未実施である。今後検討すべき項目については、タイムビジネス推進協議会実証実験分科会などと連携して様々な検討を行う予定である。

電子時刻認証システムの開発は残念ながら遅れ気味であるが、総務省及びタイムビジネス推進協議会など関係機関との協力の下に早期に電子時刻認証システムを実用化していく必要がある。

参考文献

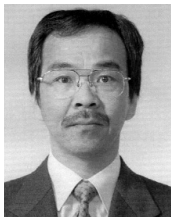
1　タイムビジネス研究会，“タイムビジネスの普及に向けて　標準時配信･時刻認証サービスの研究開発に関する研究会～タイムビジネス研究会～報告書”，平成14年6月．

2　今村，後藤，栗原，今江，岩間，“電子時刻認証システムへの日本標準時供給と評価基礎実験”，2003年信学総大，D-9-5，2003．

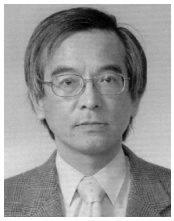
3　タイムビジネス推進協議会，“時刻認証基盤ガイドライン”，平成15年3月．

その他参考として、タイムビジネス推進協議会のホームページ
http://www.scat.or.jp/time/index.html

岩間　司
電磁波計測部門タイムスタンププラットフォームグループ主任研究員
時間周波数標準、移動通信
iwama@crl.go.jp



栗原則幸
電磁波計測部門日本標準時グループリーダー
周波数標準、空間計測
kurihara@crl.go.jp



今江理人
電磁波計測部門時間周波数計測グループリーダー
周波数標準
imae@crl.go.jp

今村國康
電磁波計測部門日本標準時グループ主任研究員
周波数標準

小竹　昇
電磁波計測部門日本標準時グループ研究員
時間・周波数標準
kotake@crl.go.jp

後藤忠広
電磁波計測部門時間周波数計測グループ研究員
GPS 時刻比較

鈴山智也
電磁波計測部門日本標準時グループ研究員　博士（工学）
時間・周波数計測
suzuyama@crl.go.jp

森川容雄
電磁波計測部門研究主管
周波数標準、時空計測
tak@crl.go.jp